IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC.,
a California Corporation,

Plaintiff,

v.

INTERNET SECURITY SYSTEMS, INC.,
a Delaware Corporation,
INTERNET SECURITY SYSTEMS, INC.,
a Georgia Corporation and
SYMANTEC CORPORATION,
a Delaware Corporation,

Defendants.

C. A. No. 04-1199 (SLR)

PUBLIC VERSION

JOINT OPENING CLAIM CONSTRUCTION BRIEF
OF DEFENDANTS ISS AND SYMANTEC

Richard L. Horwitz (#2246)
David E. Moore (#3983)
POTTER ANDERSON & CORROON LLP
Hercules Plaza 6th Floor
1313 N. Market Street
Wilmington, DE 19801
rhorwitz@potteranderson.com
dmoore@potteranderson.com

OF COUNSEL:

Holmes J. Hawkins III
Natasha H. Moffitt
KING & SPALDING LLP
191 Peachtree Street
Atlanta, GA 30303

Theresa A. Moehlman
KING & SPALDING LLP
1185 Avenue of the Americas
New York, New York 10036

Attorneys for Defendants Internet Security Systems, a Delaware Corporation and Internet Security Systems, a Georgia Corporation

Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
MORRIS JAMES HITCHENS & WILLIAMS LLP
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
rherrmann@morrisjames.com
mmatterer@morrisjames.com

OF COUNSEL:

Lloyd R. Day, Jr.
Robert M. Galvin
Paul S. Grewal
DAY, CASEBEER MADRID &
BATCHELDER LLP
20300 Stevens Creek Blvd.
Cupertino, CA 95014

Michael J. Schallop
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

Attorneys for Defendant Symantec Corporation

Dated: June 9, 2006
Public Version Dated: June 20, 2006

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

I. INTRODUCTION

Pursuant to the Court's June 30, 2005 Scheduling Order, Defendants Internet Security Systems, Inc., a Delaware corporation, Internet Security Systems, Inc., a Georgia corporation (collectively "ISS") and Symantec Corporation ("Symantec") submit this opening claim construction brief. In an effort to reduce the issues before the Court, Defendants have agreed to jointly adopt the same constructions. Each of these constructions had been previously proposed by either ISS or Symantec in the Joint Claim Construction Statement (D.I. 174). Defendants discuss the claim terms for which there is a dispute with Plaintiff SRI International, Inc. ("SRI"). The Joint Claim Chart includes additional terms on which SRI and the Defendants have essentially agreed on the proper construction to read to the jury.

At issue in this lawsuit are four related patents assigned SRI: U.S. Patent Nos. 6,484,203 ("'203 patent"), 6,711,615 ("'615 patent"), 6,321,338 ("'338 patent") and 6,708,212 ("'212 patent") (attached at Moore Decl.[1] Exs. A-D). All four patents claim priority from the same application and share an almost identical written description.[2] The first application from which all patents claim priority was filed on November 9, 1998.

These patents generally relate to detecting attacks in networked computing environments, a field known as intrusion detection.

[1] All exhibits are attached to the Declaration of David E. Moore in Support of Joint Opening Claim Construction Brief of Defendants ISS and Symantec, filed contemporaneously herewith. For convenience, those exhibits are hereafter referred to as "Ex. __."

[2] The differences among the specifications are in the summary sections.

II. BACKGROUND ON THE INTRUSION DETECTION FIELD

Early computers were standalone systems. Ensuring their security was a matter of limiting physical access to the computer. (Ex. E at p. 32 [Staniford Expert Report].) Over time, computing environments changed from the use of an isolated standalone system to a centralized mainframe accessed by user terminals to a networked environment of minicomputers and personal computers (Ex. F at p. 5 [Smaha Expert Report].) Manufacturers such as IBM, Xerox and Digital Equipment developed proprietary communication standards for their own computers. (*Id.*) In the mid-1980s, standard communication protocols were adopted for heterogeneous computers to talk to one another, leading to the rise of networked environments and the Internet. (*Id.*)

These protocols specify the format of a "network packet", the unit that is transmitted over the "wires" of a networked environment. These packets include information such as source computer address and destination computer address so that the packet can be routed across the Internet. They also include an indication of the application being used (e.g., web-based HTTP application) and any data being transported in the packet. Because the information is put into a standard format, each computing component knows where to look to find needed information. (Ex. E at pp. 10-17 [Staniford Expert Report].)[3]

Networked computing environments are insecure. As the patent states, "the very interoperability and sophisticated integration of technology that make networks such valuable assets also make them vulnerable to attack." (Ex. A ['203 patent, col. 1:37-

[3] A more detailed tutorial on the communication protocols is provided in the expert report of Stuart Staniford. (Ex. E, pp. 5-23 [Staniford Expert Report].)

39].) Potential intruders (hackers) can gain unauthorized access to an organization's computing environment by exploiting known vulnerabilities. An early example occurred when guest accounts with default passwords were a popular means of accessing an organization's computing environment. Hackers would scan the machines on that network and try to login using popular default logins and passwords. (Ex. E at p. 33 [Staniford Expert Report].)

The origin of the intrusion detection field is generally considered to be a 1980 paper by Jim Anderson, which discusses the possibility of automated intrusion detection. (*Id.* at 34.) Early intrusion detection systems were developed in the 1980s. For example, SRI worked on IDES (Intrusion Detection Expert System) and NIDES (Next-Generation Intrusion Detection Expert System), which included the development of a statistical algorithm and rule-based (also known as "signature-based") expert system for detecting anomalous behavior. (*Id.*) IDES and NIDES looked at data from audit trails or logs kept by a computer. [redacted]

Other early work was done at University of California Davis ("UC Davis"), which developed the first network intrusion detection system, NSM (Network Security Monitor), to look directly at network packets. Like IDES and NIDES, NSM used statistical and rule-based expert system technology to analyze the data. DIDS (Distributed Intrusion Detection System) was then developed to provide a centralized management platform for a set of NSMs. NSMs could send alerts to DIDS, which would combine them and perform further correlation on those alerts in an effort to detect more widespread intrusion attempts. (Ex. E at pp. 45-50 [Staniford Expert Report].)

In the mid-1990s, the Defense Advanced Research Projects Agency (DARPA) funded several projects on intrusion detection, including the GrIDS project out of UC Davis and the JiNao project out of North Carolina State University and an associated company, MCNC. (*Id.* at 56.) During this timeframe, commercial intrusion detection systems such as NetRanger, NetStalker and the RealSecure system of defendants ISS were on sale.

In late 1996, SRI received government funding for its EMERALD work, which was a follow-on to the IDES/NIDES work and led to the filing of the applications of the patents-in-suit. There are two main facets to the patents-in-suit: (1) an architecture for hierarchical event monitoring and analysis in an enterprise network and (2) a statistical algorithm for use in detecting attacks. The '203 and '615 patent claims focus on the architecture; the '338 patent claims focus on the statistical algorithm and the '212 patent claims include both. Each facet is discussed in turn after the section on claim construction law.

III. CLAIM CONSTRUCTION LAW

Claims terms "are generally given their ordinary and customary meaning," that is, "the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312-13 (Fed. Cir. 2005) (en banc), *cert. denied*, 126 S. Ct. 1332 (2006). "Importantly, the person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification." *Id.* at 1313.

"[T]he specification 'is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.'" *Id.* at 1315 (quoting *Vitronics Corp.* v. *Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)).

"Although claims need not be limited to the preferred embodiment when the invention is more broadly described, 'neither do the claims enlarge what is patented beyond what the inventor has described as the invention.'" *Inpro II Licensing* v. *T-Mobile USA Inc.*, No. 05-1233, 2006 U.S. App. LEXIS 11675, at *10 (Fed. Cir. May 11, 2006) (citation omitted). "In general, the scope and outer boundary of claims is set by the patentee's description of his invention." *On Demand Machine Corp.* v. *Ingram Indus. Inc.*, 442 F.3d 1331, 1340 (Fed. Cir. 2006) (citation omitted). "[T]he claims cannot be of broader scope than the invention that is set forth in the specification." *Id.* at 1340; *see also Phillips*, 415 F.3d at 1315-16.

Moreover, "the specification may reveal a special definition given to a claim term by the patentee that differs from the meaning it would otherwise possess. In such cases, the inventor's lexicography governs." *Phillips,* 415 F.3d at 1316. "Even when guidance is not provided in explicit definitional format, the specification may define claim terms by implication such that the meaning may be found in or ascertained by a reading of the patent documents." *Irdeto Access, Inc.* v. *Echostar Satellite Corp.*, 383 F.3d 1295, 1300 (Fed. Cir. 2004) (citation omitted).

"In other cases, the specification may reveal an intentional disclaimer, or disavowal, of claim scope by the inventor. In that instance as well, the inventor has dictated the correct claim scope, and the inventor's intention, as expressed in the specification, is regarded as dispositive." *Phillips,* 415 F.3d at 1316. "[W]hen the scope of the invention is clearly stated in the specification, and is described as the advantage and distinction of the invention, it is not necessary to disavow explicitly a different scope." *On Demand Machine Corp.*, 442 F.3d at 1340.

The Court can also consider the patent's prosecution history if it is in evidence. *Phillips,* 415 F.3d at 1317. Here, there was little dialogue between the U.S. Patent Office and the applicant during the prosecution that is of any significance to claim construction.

"[E]xtrinsic evidence, which 'consists of all evidence external to the patent and prosecution history, including expert and inventor testimony, dictionaries and learned treatises,'" may also be consulted. *Id.* (quoting *Markman* v. *Westview Instr., Inc.*, 52 F.3d 967, 980 (Fed. Cir. 1995), *aff'd*, 517 U.S. 370 (1996)). "[W]hile extrinsic evidence can shed useful light on the relevant art, ... it is less significant than the intrinsic record in determining the legally operative meaning of claim language." *Id.* at 1317 (citation omitted).

IV. THE HIERARCHICAL ARCHITECTURE CLAIMS

A. The Analysis Hierarchy Disclosed In The Specification

The patents-in-suit attempt to address the problem of recognizing attempts to infiltrate or destroy connectivity across an ***enterprise network.*** (Ex. A ['203 patent, col. 2:56-62].) Figure 1 of the patents illustrates an enterprise network:

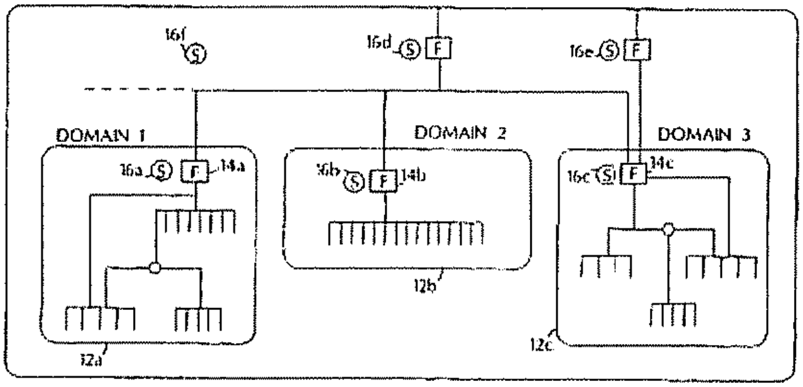


FIG. 1

The enterprise network in Figure 1 comprises three domains, each of which "includes one or more computers offering local and network services that provide an interface for requests internal and external to the domain". (*Id.* at col. 2:41-44.) [redacted] "Network services include features common to many network operating systems such as mail, HTTP, FTP, remote login, network file systems, finger, Kerberos, and SNMP." (Ex. A at col. 2:41-45 ['203 patent].)

The specification discloses "a framework for the recognition of more global threats to interdomain connectivity" that is made up of an analysis hierarchy of ***monitors*** (also called ***network monitors*** in the patent specification). The ***monitor*** is the basic building block of the hierarchical architecture. Each monitor consists of a generic code-base. (*Id.* at col. 10:29-33.)

When the generic monitors are dynamically deployed in the enterprise network, they are configured with a resource object that specifies the types of data (events) the monitor will analyze (e.g., network packet data or reports from other monitors), the parameters of the analysis that will be performed on those events, the response policies to be implemented by the monitor and a list of other monitors to send reports of suspicious activity. (*Id.* at col. 10:52-col. 11:61.) In this way, the monitors are configured to analyze and respond to network activity and to interoperate to form the analysis hierarchy. (*Id.* at col. 2:56-59.)

The preferred embodiment disclosed in the patent consists of a three-layered hierarchy: "service monitors" (16(a)-16(c) in Figure 1) that analyze data from network packets handled by a network entity; "domain monitors" (16(d)-16(e) in Figure 1) that correlate intrusion reports generated by one or more service monitors in a domain; and "enterprise monitors" (16(f) in Figure 1) that correlate reports produced across the set of monitored domains. (*Id.* at col. 2:56-col. 4:4.)

In addition, each monitor includes a "subscription list," which "enables transmission or reception of messages that report malicious or anomalous activity between monitors." (*Id.* at col. 11:49-52.) "As a monitor 16a-16f produces analysis reports, the monitor 16a-16f disseminates these reports asynchronously to subscribers. Through subscription, monitors 16a-16f distributed throughout a large network are able to efficiently disseminate reports of malicious activity." (*Id.* at col. 3:16-21.)

1. "Monitor" -- The Building Block Of The Analysis Hierarchy

As the patent specification discloses, all monitors are made up of the same code-base that is configurable by a "resource object":

> "All monitors (service, domain, and enterprise) 16a-16f use the **same monitor code-base**. However, monitors may include different resource

> objects 32 having different configuration data and methods." (*Id.* at col. 10:29-33 (emphasis added).)
>
> "The resource object 32 provides a pluggable configuration module for tuning the **generic monitor code-base** to a specific event stream." (*Id.* at col. 10:52-58 (emphasis added).)

According to the patent, an advantage of this reusable software architecture is that it "can reduce implementation and maintenance efforts. Customizing and dynamically configuring a monitor 16 thus becomes a question of building and/or modifying the resource object." (*Id.* at col. 10:33-37.) "A library of resource objects 32 provides prefabricated resource objects 32 for commonly available network entities." (*Id.* at col. 10:48-51.)

As SRI's expert testified, "[a]rchitecturally, the patent specification does teach using the same general architecture for the hierarchical monitor as it does for the network service monitor." (Ex. I at p. 524 [Kesidis deposition].) In Figure 2 of the patent, which is reproduced below, the monitor is shown within the dotted box (which we have outlined

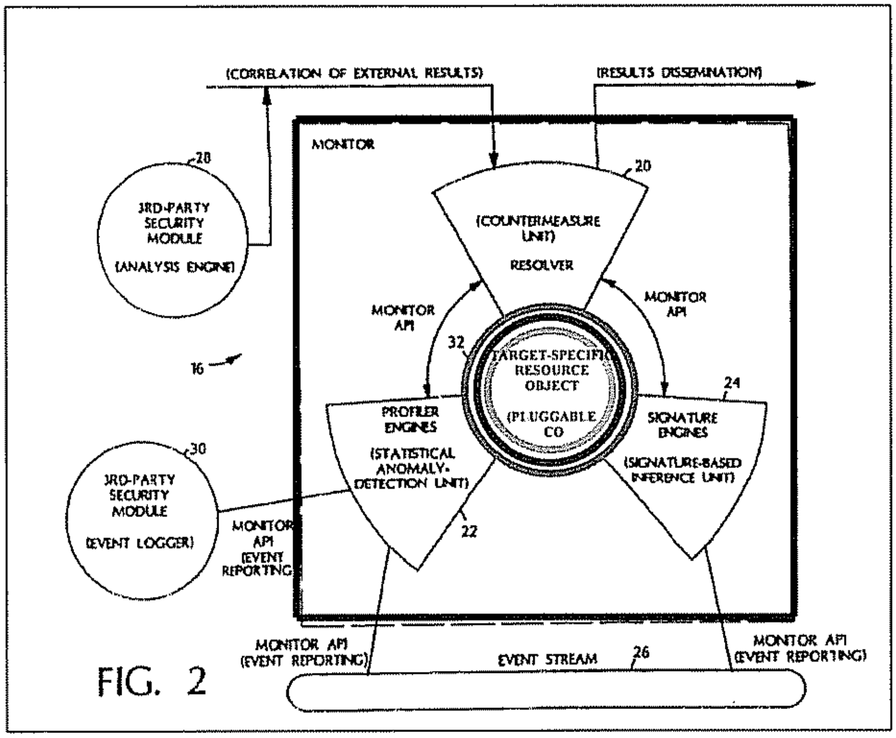
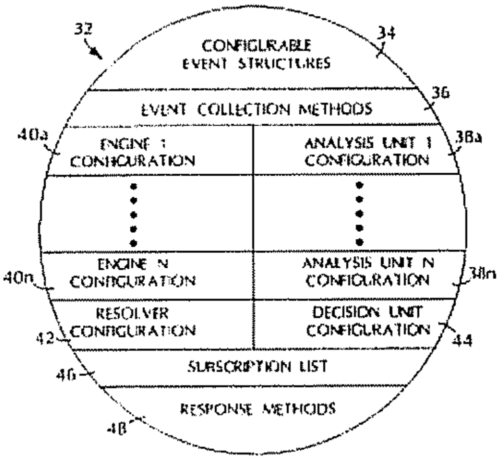

(CORRELATION OF EXTERNAL RESULTS)
(RESULTS DISSEMINATION)
MONITOR
28
3RD-PARTY SECURITY MODULE (ANALYSIS ENGINE)
20
(COUNTERMEASURE UNIT)
RESOLVER
MONITOR API
MONITOR API
32
TARGET-SPECIFIC RESOURCE OBJECT (PLUGGABLE CO
16
24
PROFILER ENGINES (STATISTICAL ANOMALY-DETECTION UNIT)
SIGNATURE ENGINES (SIGNATURE-BASED INFERENCE UNIT)
30
3RD-PARTY SECURITY MODULE (EVENT LOGGER)
MONITOR API (EVENT REPORTING)
22
MONITOR API (EVENT REPORTING)
EVENT STREAM
26
MONITOR API (EVENT REPORTING)

FIG. 2

in purple). The monitor is configured with a target-specific resource object, which is shown as the circle in the center of the box. We have added three colored circles to indicate that resource object can take on different forms. The patent discloses that "each monitor 16 includes one or more analysis engines 22, 24. These engines 22, 24 can be dynamically added, deleted, and modified as necessary. In the dual-analysis configuration shown, a monitor 16 instantiation includes a signature analysis engine 22 [sic 24] and a statistical profiling engine 24 [sic 22]. ... A monitor 16 also includes a resolver 20 that implements a response policy and a resource object 32 that configures the monitor 16." (*Id.* at col. 4:5-15.)

As shown in Figure 2, "[e]ach monitor 16 can analyze event records that form an event stream. The event stream may be derived from a variety of sources such as TCP/IP network packet contents or event records containing analysis reports disseminated by other monitors." (*Id.* at col. 4:18-22.) Because the monitor receives data in this abstracted format of events, the same monitor code-base can be configured and reconfigured to act at any layer in the hierarchy.

The pluggable ***resource object*** that configures the monitor is shown in Figure 3 of the patents, reproduced below. The various elements of the resource object are used to configure the monitor into a specific type of monitor. For example, a monitor's input (events) is configured by the "configurable event structures" 34. The event stream can include network packet data or reports from other monitors. "Event-collection methods 36 gather and parse event records for analysis engine processing." (*Id.* at 11:5-6.) Because the format of the input to monitor is a structured "event", the generic monitor



code-base can be configured to operate at any layer in the hierarchy, whether receiving network packet data at a lower layer or reports from other monitors at a higher layer:

> "The monitor code-base maintains no internal dependence on the content or format of any given event stream or the analysis results produced from analyzing the event stream. Rather, the resource object 32 provides a universally applicable syntax for specifying the structure of event records and analysis results." (*Id.* at col. 10:59-66.)

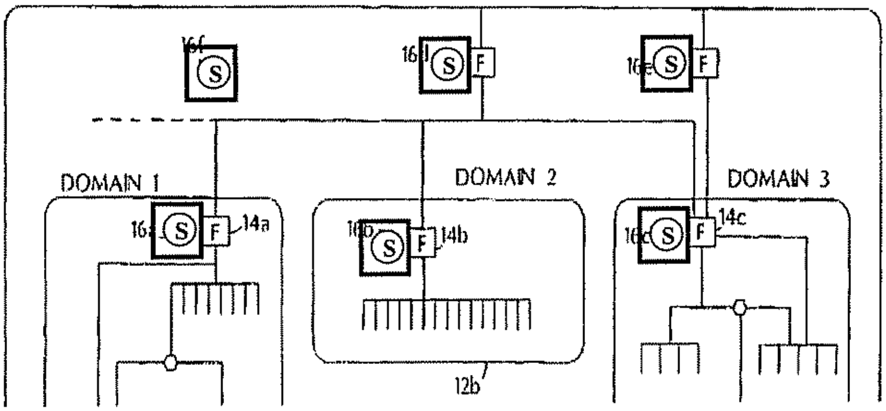
The resource object also includes configuration variables for the analysis engines that process the events: "Processing by analysis engines is controlled by engine configuration 40a-40n variables and data structures that specify the operating configuration of a fielded monitor's analysis engine(s)." (*Id.* at col. 11:5-9.) The analysis unit configurations "include configuration variables that define the semantics employed by the analysis engine to process the event stream." (*Id.* at col. 11:12-14.)

As shown in Figure 3, the resource object also includes configuration variables for merging the analysis results via the monitor's resolver. "The resolver configuration 42 includes operating parameters that specify the configuration of the resolver's internal modules. The decision unit configuration 44 describes semantics used by the resolver's decision unit for merging the analysis results from the various analysis engines. These semantics include the response criteria used to invoke countermeasure handlers. A resource object 32 may also include response methods 48." (*Id.* at col. 11:15-24.) As the patent discloses, "[c]ountermeasures range from very passive responses, such as report dissemination to other monitors 16a-16f or administrators, to highly aggressive actions, such as severing a communication channel or the reconfiguration of logging facilities within network components." (*Id.* at col. 11:33-37.)

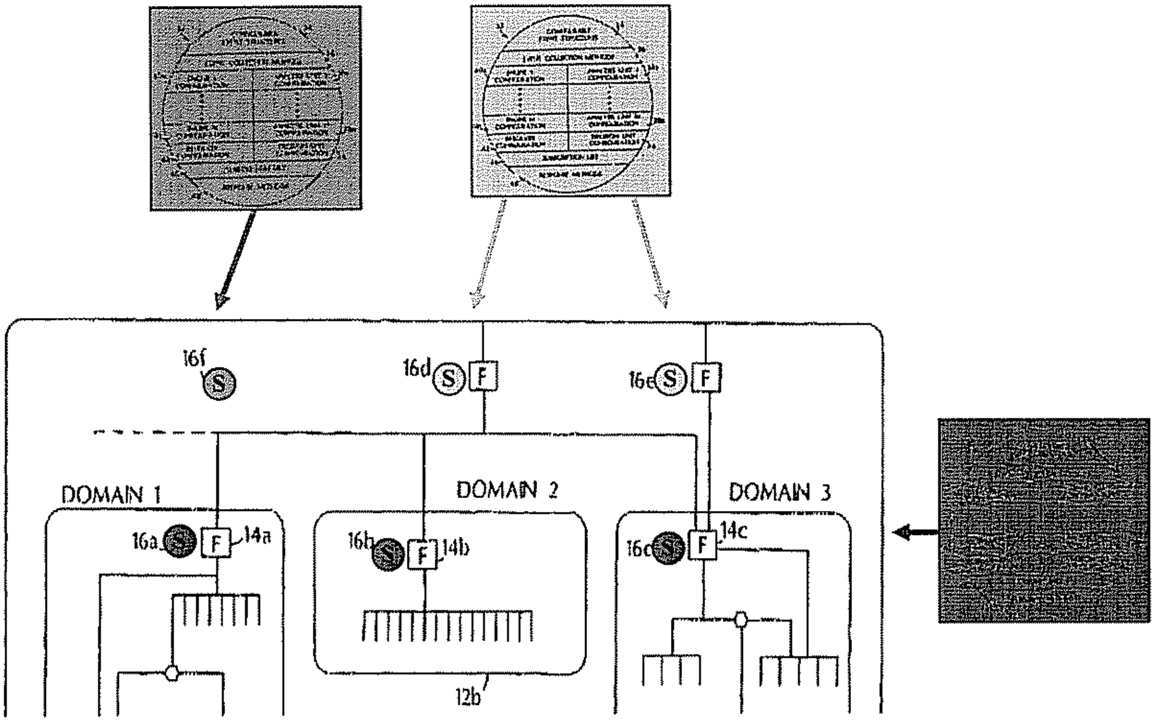
Finally, the resource object includes the subscription list for the monitor. This mechanism is used to build the analysis hierarchy by creating a reporting structure for the monitors: "Upon its initialization, the resolver 20 initiates authentication and subscription sessions with those monitors 16a-16f whose identities appear in the monitor's 16 subscription list." (*Id.* at col. 7:54-58.)

2. Deploying The Monitors In The Analysis Hierarchy

Figure 1 has been annotated to show how, using resource objects, generic monitors can be dynamically deployed. (*Id.* at col. 2:56-57.) Generic monitors are represented in yellow. Through configuration with a resource object, the monitor takes



its form as a service monitor (red); domain monitor (blue) or enterprise monitor (green), as shown in the annotated figure below. The service monitors (red) can be configured to report to one or more domain monitors (blue), and the domain monitors (blue) can be configured to report to one or more enterprise monitors (green). Additionally, as discussed in the patent specification, monitors at the same layer in the hierarchy can also form "peer-to-peer" relationships where they subscribe to each others reports. (*Id.* at col. 3:2-36.)



Because the monitor consists of a generic code-base configured by a resource object, the monitor can be reconfigured by reconfiguring the elements of the resource object:

> "The contents of the resource object 32 are defined and utilized during monitor 16 initialization. In addition, these fields may be modified by internal monitor 16 components, and by authorized external clients using the monitor's 16 API. Modifying the resource object 32 permits adaptive analysis of an event stream ...." (Ex. A at col. 11:62-67 ['203 patent].)

Thus, the architecture of monitors allows for adapting the analysis simply by modifying the fields of the resource object.

3. The Lack Of Disclosure On "Correlation" By Higher Level Monitors

While much of the specification concerns the generic monitor architecture, little is disclosed as to ***what*** the hierarchical monitors do with the reports produced by the lower-level monitors. SRI's expert, George Kesidis, confirmed the lack of disclosure in the patent specification at his deposition: "The actions of the network service monitors are described in greater detail." (Ex. I at pp. 124-25 [Kesidis Dep.].) As Professor Kesidis admitted, the patent fails to disclose how the disclosed analysis engines could be configured to act at the hierarchical monitor level:

> "The Witness: How to apply a statistical algorithm?
>
> The details in the specification of the patent regarding the processing of reports of suspicious activity and issuing meta alerts are much less than the corresponding description of the internal operations of a network service monitor. There isn't as much detail." (*Id. at* 125.)
>
> "Q. Is there anything in this patent specification that discloses examples of where a hierarchical monitor using a signature engine could be used?
>
> A. An example, a specific example of a hierarchical monitor, the specific functioning of a hierarchical monitor is not directly given, I don't think, in the patent spec." (*Id. at* 127.)

And, as Professor Kesidis admitted, common techniques for hierarchical correlation analysis were not known at the time:

> "Q. I'll ask it in the positive way to make it clear. Were there commonly known techniques in the art, in the intrusion detection field, in November of 1998 that implemented hierarchical correlation?
>
> A. In this context? No. I don't believe there were." (*Id. at* pp. 129.)

Frank Jou, a principal investigator on the prior art JiNao system, gave similar testimony at his deposition regarding the lack of common techniques for hierarchical analysis:

> "[C]ollect[ion] of the local detection results was not an issue. The issue was how do you come up with the intelligence, how do you correlate all the relevant information and be able to, you know, derive a certain logical or reasonable conclusion. ... So that was, you know, the open question at that point." (Ex. K at pp. 172-73 [Jou Dep.].)

The patent specification does not solve, or suggest how to solve, the open question.

The specification merely discloses collecting, or aggregating the reports, at the hierarchical level.

> "Above the service layer, signature engines 24 scan the aggregate of intrusion reports from service monitors in an attempt to detect more global coordinated attack scenarios or scenarios that exploit interdependencies among network services." (Ex. A at col. 6:58-62 ['203 patent].)

The most the patent specification offers is that a particular measure class, called event measures, may be useful for correlation, but the specification again fails to describe how one might actually implement such an event measure at the hierarchical level. (Ex. A, col. 5:51-62 ['203 patent].)

Thus, while the specification contemplates correlating reports at a higher level monitor, it provides no details on how to actually perform such an analysis.

B. The Asserted Hierarchical Architecture Claims

Of the claims SRI has asserted in this lawsuit, the following contain limitations relating to the hierarchical architecture disclosed in the patent:

Patent	**Claims asserted against Symantec**	**Claims asserted against ISS**
'203 patent	1-9, 11-20, 22	1-2, 4-6, 12-13, 15-17

'615 patent	1-10, 12-21, 23, 34-41, 43, 44-51, 53	1-2, 4-6, 13-14, 16-18
'212 patent	1-11, 13-22, 24	[ISS's Declaratory Judgment Action includes this patent]
'338 patent	12-15	12-13

The structure of the hierarchical architecture claims is similar across the patents.

Claim 1 of the '203 patent provides an example (terms to be construed in bold):

> 1. A computer-automated method of **hierarchical event monitoring and analysis** within an enterprise network comprising:
>
> **deploying a plurality of network monitors in the enterprise network**;
>
> detecting, by the **network monitors**, suspicious network activity based on analysis of network traffic data **selected from** the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet};
>
> generating, by the monitors, reports of said suspicious activity; and
>
> **automatically receiving and integrating the reports of suspicious activity**, by one or more **hierarchical monitors**.

1. Monitor/Network Monitor

Term	Defendants' Construction
network monitor monitor	Generic code that can be dynamically configured and reconfigured with reusable modules that define the monitor's inputs, analysis engines and their configurations, response policies and output distribution for its reports.

The term ***monitor*** did not have a well-known meaning in the art at the time the patent specification was filed. (Ex. F at pp. 19-20 [Smaha Expert Report].) Therefore, one of skill in the art would need to look to the definition provided in the patent. "[I]f a disputed term has no previous meaning to those of ordinary skill in the prior art, its meaning, then, must be found elsewhere in the patent." *Irdeto Access,* 383 F.3d at 1300 (citation omitted). "[A]bsent such an accepted meaning, we construe a claim term only as broadly as provided for by the patent itself. The duty thus falls on the patent applicant to provide a precise definition for the disputed term." *Id.* Here, the patentee defined monitor, a term that had no previous meaning in the art, as a particular software architecture.

As disclosed in the specification, the monitor is the basic building block of the hierarchical event monitoring and analysis method of the patent. The monitor consists of generic code that can be dynamically configured and reconfigured with a resource object. (Ex. A at col. 10:29-33 and 10:52-58 ['203 patent].) That resource object provides the configuration information for a monitor -- what data it will take as input; the configurations of its analysis engines; any response policies it will implement; and the other monitors to which it will provide its analysis reports. Through this mechanism, the generic monitor can be configured to operate at any layer in the hierarchy. In addition, as disclosed in the patent, the monitor can be reconfigured by modifying the elements of the resource object. (*Id.* at col. 11:62-67.) As the patent discloses, such reconfiguration allows for adapting the analysis. (*Id.*)

Defendants' construction is the definition of monitor in the patent specification. "[T]he specification is 'the single best guide to the meaning of a disputed term,' and ... 'acts as a dictionary when it expressly defines terms used in the claims or when it defines terms by implication.'" *Phillips*, 415 F.3d at 1321 (citing *Vitronics*, 90 F.3d at 1582).

Here, the specification defines ***monitor*** to have the configurable, reusable software architecture reflected in Defendants' construction.

According to the specification, this reusable software architecture has many advantages. It enables an analysis hierarchy to be formed, providing "a framework for the recognition of more global threats to interdomain connectivity, including coordinated attempts to infiltrate or destroy connectivity across an enterprise network." (Ex. A, col. 2:58-63 ['203 patent].) It allows reuse of modules, which the patent specification states "reduce[s] implementation and maintenance efforts." (*Id.* at col. 10:33-37 and 10:48-51.) Finally, the monitor can be easily reconfigured, which allows for adaptive analysis. (*Id.* at col. 11:62-67.)

Thus, this reusable software architecture of monitors is what SRI perceived as the invention. "[W]hen the scope of the invention is clearly stated in the specification, and is described as the advantage and distinction of the invention, it is not necessary to disavow explicitly a different scope." *On Demand Machine Corp.*, 442 F.3d at 1340.

Accordingly, the proper construction for ***monitor*** is the definition the patentee put forth in the patent specification, which is reflected in Defendants' proposed construction.

SRI's Proposed Construction of Monitor/Network Monitor Has No Bearing To The Description Of The Alleged Invention In The Specification

SRI's construction of the claim terms relating to monitor are so broad as to encompass any component -- software, hardware or otherwise -- that can analyze data:

Term	**SRI's Construction**
network monitor monitor	Process or component in a network that can analyze data; depending on the context in specific claims, the network monitor may analyze network traffic data, reports of suspicious network activity or both. Service

	monitors, domain monitors and enterprise monitors are examples of network monitors.

This type of construction, which ignores the definition provided in the specification, has the overbreadth that the Federal Circuit recently warned against: "The problem is that if the district court starts with the broad dictionary definition in every case and fails to fully appreciate how the specification implicitly limits that definition, the error will systematically cause the construction of the claim to be unduly expansive." *Phillips*, 415 F.3d at 1321.

As discussed above, the patent specification defines monitor as having the software architecture of a generic code-base that can be configured with a reusable module. That monitor architecture provides for the building of an analysis hierarchy, eases maintenance and allows for reconfiguration. SRI's construction of monitor fails to specify how that monitor could achieve any of these stated goals. It, therefore, is incorrect. *See Netword, LLC* v. *Centraal Corp.*, 242 F.3d 1347, 1352 (Fed. Cir. 2001) ("The claims are directed to the invention that is described in the specification; they do not have meaning removed from the context from which they arose. Thus the claims are construed to state the legal scope of each patented invention, on examination of the language of the claims, the description in the specification, and the prosecution history.")

2. Specific Types of Monitors

Term	Defendants' Construction
hierarchical monitor	a *network monitor* that receives reports as input from one or more network monitors that are at a lower layer

hierarchically higher network monitor	in the analysis hierarchy
service monitor	a *network monitor* that provides local real-time analysis of network packets handled by a network entity
domain monitor	a *network monitor* that receives and analyzes intrusion reports disseminated by *service monitors*
enterprise monitor	a *network monitor* that receives and analyzes intrusion reports disseminated by *domain monitors*

As discussed above, the preferred embodiment disclosed in the specification includes a three-tiered hierarchy of monitors -- service monitors that feed domain monitors that, in turn, feed enterprise monitors. (Ex. A at col. 2:56 to 4:4 [‘203 patent].) This defined hierarchy is reflected in Defendants' construction. Similarly, a hierarchical monitor, as set forth in the specification, is a monitor that receives analysis reports from monitors at a lower layer in the hierarchy.

SRI's Proposed Construction

SRI's constructions of the other monitor terms similarly ignore the specification:

Term	**SRI's Construction**
hierarchical monitor hierarchically higher network monitor	Process or component in a network that receives reports from at least one lower-level monitor.
service monitor	SRI does not believe the term needs construction but, if construed, should be construed to mean a network monitor that analyzes data from individual components or services.

domain monitor	SRI does not believe the term needs construction but, if construed, should be construed to mean a network monitor that analyzes data from a domain.
enterprise monitor	SRI does not believe the term needs construction but, if construed, should be construed to mean a network monitor that analyzes data from an enterprise, i.e. a collection of domains.

Here, SRI's proposals are particularly egregious. Service, domain and enterprise monitors are terms from the preferred embodiment. They do not have meaning outside of the specification.

The specification is clear -- service monitors analyze traffic data and feed domain monitors; domain monitors feed enterprise monitors. This notion of the defined hierarchy is completely absent from SRI's constructions. SRI's constructions are therefore incorrect.

3. Terms Relating To Deploying An Analysis Hierarchy Of Monitors

Term	**Defendants' Construction**
hierarchical event monitoring and analysis	monitoring and analyzing events through the use of network monitors that are configured to form an analysis hierarchy of two or more layers
deploying a plurality of network monitors	installing and configuring two or more network monitors so that together they form an analysis hierarchy defined by the network monitors' inputs and output distribution

Many of the hierarchical claims in the preamble call for a method of ***hierarchical event monitoring and analysis.*** As discussed above, this method is defined in the patent as monitoring and analyzing events via the analysis hierarchy of monitors.

With respect to the ***deploying*** step, Defendants' construction reflects the definitions in the patents pertaining to how to build an analysis hierarchy of monitors. The patent shows an enterprise network that includes "dynamically deployed network monitors 16a-16f that analyze and respond to network activity and can interoperate to form an analysis hierarchy." (Ex. A at col. 2:56-59 ['203 patent].) As the patent teaches, monitors are made up of a generic code-base, and deploying a monitor includes dynamically configuring the monitor with the reusable module:

> "All monitors (service, domain, and enterprise) 16a-16f use the same monitor code-base. However, monitors may include different resource objects 32 having different configuration data and methods. This reusable software architecture can reduce implementation and maintenance efforts. Customizing and dynamically configuring a monitor 16 thus becomes a question of building and/or modifying the resource object 32." (*Id.* at col. 10:29-37.)

See also id. at col. 10: 52-54 ("The resource object 32 provides a pluggable configuration module for tuning the generic monitor code-base to a specific event stream.").

These constructions, like the monitor construction, result from the description of the claimed invention in the patent specification. Under the patent statute, a patentee is to "provide a 'full' and 'exact' description of the claimed invention" and, therefore, "the specification necessarily informs the proper construction of the claims." *Phillips*, 415 F.3d at 1316. Defendants' constructions stay true to the claim language and naturally align with the patent's description of the analysis hierarchy of monitors. Those constructions, therefore, are the correct constructions. *Renishaw PLC* v. *Marposs Societa' per Azioni,* 158 F.3d 1243, 1250 (Fed. Cir. 1998) (citations omitted).

SRI's Proposed Constructions

SRI's constructions of the terms relating to the deployment of monitors in the analysis hierarchy provide no construction at all:

Term	SRI's Construction
hierarchical event monitoring and analysis	monitoring events through the use of a hierarchical monitor
deploying a plurality of network monitors	SRI does not believe the term needs construction but, if construed, should be construed to mean locating two or more network monitors so as to allow them to receive data to be monitored and/or to send information.

SRI's proposed construction of hierarchical event monitoring and analysis is divorced from the specification. Deploying the monitors defined in the specification involves configuring them so that together they form an analysis hierarchy. (Ex. A at col. 2:56-65 ['203 patent].) The specification envisions that such an analysis hierarchy of monitors can be of any depth or breadth and specifically teaches that centralizing an analysis is to be avoided: "The enterprise monitor 16f (or monitors, as it would be important to avoid centralizing any analysis)." (*Id.* at col. 3:55-56.)

SRI seeks to avoid using the definitions set forth in the patent specification. SRI's constructions seek to encompass any process or component that analyzes data; however, it fails to specify how such process or components could perform the hierarchical event monitoring and analysis of the patent. The SRI patents disclose and define a specific architecture to perform hierarchical event monitoring and analysis as the alleged invention. SRI cannot now attempt to reach architectures that it did not describe as the invention. *On Demand Machine*, 442 F.3d at 1338 (Fed. Cir. 2006) ("the claims cannot be of broader scope than the invention that is set forth in the specification.")

4. Terms Relating To Analysis At The Hierarchical Level

Term	**Defendants' Construction**
automatically receiving and ***integrating*** the reports of suspicious activity, [by one or more hierarchical monitors]	automatically receiving and combining the reports of detected suspicious network activity
Dependent claims: wherein integrating comprises ***correlating*** intrusion reports reflecting underlying commonalities	determining relationships among the reports of detected suspicious network activity

The term ***integrating*** does not appear anywhere in the specification. Moreover, while the patent discloses that hierarchical monitors are supposed to ***correlate*** reports, there is no description of how such ***correlation*** is to be done. The term ***correlation*** has a statistical definition, however, that is not the intended meaning of the term in the patent specification. (*See, e.g.*, Ex. I at p. 230 [Kesidis Dep.] ("The word 'correlation' is a well-defined statistical term", however, "I don't think in this particular claim that there is necessarily a statistical meaning breathed into the word 'correlation.'"); *see also* Ex. F at pp. 20-21 [Smaha Expert Report].)

Where, as here, there is no definition of the term in the patent specification and there is no reasonably attributed technical meaning, it is appropriate to apply the general definition of the term. "Dictionaries or comparable sources are often useful to assist in understanding the commonly understood meaning of words and have been used both by our court and the Supreme Court in claim interpretation." *Phillips*, 415 F.3d at 1322; *see also Free Motion Fitness, Inc.* v. *Cybex Int'l., Inc.*, 423 F.3d 1343, 1348-49 (Fed. Cir. 2005).

Accordingly, Defendants draw on dictionary definitions for their claim constructions of integrating and correlating. The relevant dictionary definitions of ***integrate*** are

> "1. to bring together or incorporate (parts) into a whole. 2. to make up, combine, or complete to produce a whole or a larger unit, as parts do. 3. to unite or combine." (Ex. L [Random House Unabridged Dictionary (2d ed. 1993].)

These definitions indicate that integrate means combining pieces together. Pursuant to this plain meaning, Defendants propose construing "***integrating*** the reports of suspicious activity" as "combining the reports of detected suspicious network activity."

The relevant dictionary definitions of ***correlate*** are

> "1. to place in or bring into mutual or reciprocal relation; establish in orderly connection: to *correlate expenses and income.* - *v.i.* 2. to have a mutual or reciprocal relation; stand in correlation: *The results of the two tests correlate to a high degree.* - *adj.* 3. mutual or reciprocally related." (*Id.*)

In accordance with these definitions, Defendants construe ***correlating*** intrusion reports reflecting underlying commonalities as "determining relationships among the reports of detected suspicious network activity."

The inventors agree that these ordinary definitions are what would have been understood as the meaning of the terms by one skilled in the art at the time the patent was filed. [redacted]

[redacted]

The testimony was similar with respect to using the ordinary meaning of "correlating." [redacted]

> [redacted]

Thus, Defendants' constructions are in accord with the ordinary meaning of the terms and with the understanding of the inventors.

SRI's Proposed Construction

Term	**SRI's Construction**
automatically receiving and ***integrating*** the reports of suspicious activity, [by one or more hierarchical monitors]	Without user intervention, receiving reports and combining those reports into another functional unit.
Dependent claims: wherein integrating comprises ***correlating*** intrusion reports reflecting underlying commonalities	Combining the reports based on underlying commonalities between them.

SRI's constructions are similar to Defendants' constructions. However, SRI seeks to add a requirement that *integrating* include the requirement that the reports be combined into another "functional unit." Nowhere does the patent specification disclose such a requirement. Rather than clarify the meaning of the claims, SRI's construction adds ambiguity -- what is a "functional unit"? Given the lack of foundation for this construction in the intrinsic record and the resulting ambiguity, SRI's construction should be rejected.

Furthermore, by simply repeating the term "commonalities" in its definition of the phrase "correlating intrusion reports reflecting underlying commonalities," SRI's construction essentially provides no additional guidance on the claim term. In addition, this claim term depends from the integrating step and it is unclear whether SRI's construction on correlation includes the requirement that the reports be combined into "another functional unit." Therefore, Defendants' constructions of integrate and correlate, where the correlating step adds to the integrating step, is preferable.

V. THE STATISTICAL DETECTION CLAIMS

A. Background and Disclosure Relating to Statistical Detection

The patents-in-suit generally describe two categories of intrusion detection methods -- statistical detection (also known as "anomaly detection") and signature detection (also known as "rule-based" or "threshold" detection). (*See* Ex. C at cols. 5:36-52, 7:23-8:13, Fig. 2 ['338 patent]; [redacted].) Both statistical detection and signature detection techniques were known years before the claimed inventions. (*See* Ex. E at pp. 34-36 [Staniford Expert Rep.], [redacted]

[redacted]; Ex. N [Valdes & Anderson, “Statistical Methods for Computer Usage Anomaly Detection Using NIDES” (Jan. 1995)].) An important distinction between these two categories of intrusion detection is that a signature detection method requires prior knowledge of suspicious network activity in order to develop a rule or “signature” for detecting such activity while a statistical detection method does not. (Ex. C at col. 7:24-26 [‘338 patent]; Ex. I at p. 477:2-12 [Kesidis Dep.]). In theory, a statistical detection method is therefore able to detect suspicious (anomalous) activity that may not have been previously observed. (Ex. C at col. 2:46-48, 6:52-7:8 [‘338 patent]; Ex. I at pp. 481:19-482:4 [Kesidis Dep.].)

The specification of the patents-in-suit provides one example of a statistical detection method for identifying suspicious network activity. This detection method involves statistical profiles that represent probability distributions of observed network activity that are aged over time.[4] A long-term statistical profile of network activity based on certain types of measures is automatically generated and updated to represent “normal activity.” (Ex. C at col. 2:42-46 [‘338 patent].) A short-term statistical profile of network activity is automatically generated to represent “recent activity.” (*Id.* at col. 6:44-47.) The short-term and long-term statistical profiles are then compared. If the difference is “significant”, this anomaly may indicate suspicious network activity. (*Id.* at col. 6:44-47; *see also* Figs. 4 and 5.) That difference will be considered “significant” when it exceeds an historically adaptive threshold that is empirically determined to be

[4] For further background and a tutorial relating to statistics as well as the relevant statistical algorithms and profiles, see Ex. E at pp. 24-31, 38-45 [Staniford Expert Rep.].

statistically significant. (*Id.* at col. 6:59-67.) This threshold is "adaptive" because it changes over time based on the history of events -- when behavior changes over time, the algorithm will adjust the threshold according to the empirical data.

According to the specification, the advantage of this method is that it requires no prior knowledge of intrusive or exceptional activity. (*Id.* at col. 6:57-58.) In other words, the administrator of the system is not required to "catalog each possible attack upon the network." (*Id.* at col. 2:46-48.) Instead, what constitutes suspicious network activity is "learned" based on observed data over time.

As the specification and the inventors have acknowledged, the statistical analysis technique of detecting suspicious activity using long-term and short-term statistical profiles was well-known years before the work described in the specification. (*Id.* at col. 5:43-49 (incorporating by reference a 1995 article describing such techniques)]; [redacted]

B. Statistical Detection Claims

All of the asserted claims of the '338 and '212 patents contain claims directed to statistical detection. Claim 1 of the '338 patent is representative of the statistical detection claims (terms to be construed in bold):

> A method of network surveillance, comprising:
>
> receiving network packets handled by a network entity;
>
> **building at least one long-term and at least one short-term statistical**

> **profile** from at least one measure of the network packets, the at least one measure monitoring data transfers, errors, or network connections;
>
> comparing at least one long-term and at least one short-term statistical profile; and
>
> **determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.**

Claim 1 of the '212 patent is another representative claim; it combines elements of hierarchical monitoring with statistical detection (statistical detection term to be construed in bold):

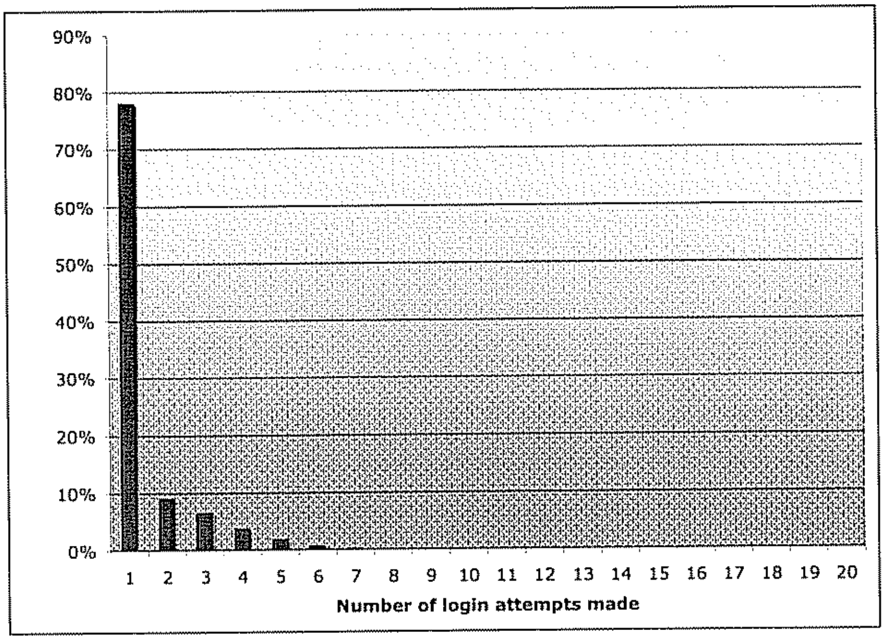
> Method for monitoring an enterprise network, said method comprising the steps of:
>
> deploying a plurality of network monitors in the enterprise network;
>
> detecting, by the network monitors, suspicious network activity based on analysis of network traffic data, wherein at least one of the network monitors utilizes a **statistical detection method**;
>
> generating, by the monitors, reports of said suspicious activity; and
>
> automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.

C. "Building at least one long-term . . . statistical profile"

Claim Term	Defendants' Proposed Construction
"building at least one long-term . . . statistical profile"	automatically generating and updating an exponentially aged probability distribution of historically observed activities

The specification makes clear that the system, not a user, automatically generates and updates the statistical profiles: "The system maintains and updates a description of behavior with respect to these measure types in an updated profile." (Ex. C at col. 6:38-39 ['338 patent].) In the only embodiment described, the profile engine 22 (also known as the "statistical anomaly detection unit") "can use a wide range of multivariate statistical measures to profile network activity indicated by an event stream." (Ex. C at col. 5:36-38 ['338 patent].)

The statistical profiles are probability distributions based on observed values. (Ex. C at cols. 5:59-61, 6:8-10, 6:54-57 ['338 patent,]; *see also* Ex. N at p. 307 [*Statistical Methods* paper] ("For each measure, we construct a probability distribution of short-term and long-term behaviors.").) A probability distribution is a well-established concept in statistics. A probability distribution is essentially a list of events that might occur and the odds that each of them will happen. (Ex. E at p. 26 [Staniford Expert Rep.].) All of the probabilities must add up to 100%, and are often visualized as a histogram. For example, a probability distribution based on the observed number of failed login attempts over the course of a day might look as follows:



In this hypothetical example, the probability distribution reflects that in 78% of the logins, the users succeeded on the first try. In 9% of the logins, the users succeeded on the second try, and so forth. (Ex. E at p. 26 [Staniford Expert Rep.].)

The specification makes clear that the statistical profiles constitute probability distributions based upon the values of the observed measures of network activity. For example, the specification describes that profiler engine 22 "allocate[es] bins appropriate to the range of values of the underlying measure, and then track[s] the frequency of observation of each value range." (Ex. C at col. 6:5-8 ['338 patent].) In other words, for a measure of network traffic like number of packets over a specified time interval (*e.g.*, 1 minute, 10 minutes, etc.), the distribution of different observed values and their frequency would be created in order to determine significant variance with past observed activity.

The building of the long-term statistical profile is described in the specification as follows:

> At update time (typically, a time of low system activity), the update function folds the short-term values observed since the last update into the long-term profile, and the short-term profile is cleared. The long-term profile is itself slowly aged to adapt to changes in subject activity. (Ex. C at col. 6:47-52 ['338 patent].)

Thus, the long-term profile is a profile of historically observed activity that is aged in order to adapt to changes in activity over time. The specification makes clear that the values in the profiles are "exponentially" aged -- i.e., the data in the profiles are exponentially weighted based on how long ago the data were collected. (Ex. C at col. 6:42-45 ['338 patent]; *see also* Ex. N at p. 306 [*Statistical Methods* paper]; Ex. O at p. 4 [*Live Traffic Analysis* paper].) In this way, more recent data carries more weight.

Based upon the definition and description of "long-term statistical profile" in the specification, Defendants propose that the limitation "building at least one long-term . . .

statistical profile" be construed to mean "automatically generating and updating an exponentially aged probability distribution of historically observed activities."

SRI's Proposed Construction

There are two significant differences between SRI and Defendants' proposed constructions for "building a long-term . . . statistical profile."[5]

First, SRI's construction lacks any express requirement that the "building" step be performed automatically by the system based on historically observed activity. SRI's construction would appear to therefore encompass instances where a user simply created a statistical description or threshold. But as shown above, the specification describes the long-term profile as being automatically generated and updated by the system, not set by a user.

Second, SRI's construction simply characterizes a statistical profile as a "statistical description." The term "statistical description," however, is not used in the specification and provides no more meaning than the claim term "statistical profile." SRI's own expert conceded it was a "broad term" that could mean a "variety of different things," and struggled to provide any clear definition. (Ex. I at pp. 330:5-331:8 [Kesidis Dep.].) The phrase "statistical description" therefore would provide little or no guidance to the jury as to what constituted a "long-term statistical profile." As shown above, the specification, however, provides a fairly detailed description of what constitutes a "long-term statistical profile." One of ordinary skill in the art would have understood the

[5] SRI has offered a construction with respect to the entirety of the limitation "building a long-term and short-term statistical profile from at least one measure of the network packets." Defendants believe it is easier to understand this limitation if the long-term and short-term statistical profiles are addressed separately. However, this is not a major substantive difference between the parties.

meaning of the term in light of the specification to require, at a minimum, that the statistical profile constitute a probability distribution of historically observed activities that is exponentially aged. Accordingly, Defendants' construction should be adopted.

D. "Building at least one . . . short term statistical profile"

Claim Term	Defendants' Proposed Construction
"building at least one. . . short-term statistical profile"	automatically generating and updating an exponentially aged probability distribution of recently observed activities

The only difference between the term "short-term statistical profile" and "long-term statistical profile" is that a "short-term statistical profile" represents recently observed activities. According to the specification,

> The short-term profile accumulates values between updates, and exponentially ages (e.g., weighs data based on how long ago the data was collected) values for comparison to the long-term profile. As a consequence of the aging mechanism, the short-term profile characterizes recent activity, where "recent" is determined by a dynamically configurable aging parameters. (Ex. C at col. 6:41-47 ['338 patent].)

In all other respects, the construction should be identical, since short-term statistical profiles, like long-term statistical profiles, are automatically generated and updated and consist of an exponentially aged probability distribution. (*Id.* at col. 5:59-61, 6:8-10, 6:42-45, 6:54-57.)

SRI's Proposed Construction

SRI agrees that a short-term statistical profile represents "recent network activity" as opposed to "historical network activity." But again, instead of providing a construction of the term "statistical profile" consistent with the specification, SRI proposes that the term be construed to mean a "statistical description." As explained above, SRI's construction fails to account for the clear description in the specification.

E. "Determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity"

Claim Term	Defendants' Proposed Construction
"determining whether the difference between the short-term statistical profile and the long-terms statistical profile indicates suspicious network activity"	determining whether the difference between the short-term statistical profile and the long-term statistical profile exceeds a threshold that is empirically determined to indicate suspicious activity based on the historically adaptive deviation between the two profiles, requiring no prior knowledge of suspicious network activity.

The specification describes the use of "mathematical algorithms . . . to assess the anomaly of events." (Ex. C at col. 5:40-43 ['338 patent].) Suspicious network activity is determined by first measuring the "distance," or difference, between the short-term and long-term profiles. (*Id.* at 6:60-63). Then, the difference between the two profiles is compared to a historically adaptive threshold that is empirically determined based on past observations:

> The difference is compared to a historical deviation. The empirical distribution of this deviation is transformed to obtain a score the event. Anomalous events are those whose scores exceed a historically adaptive score threshold based on the empirical score distribution. (*Id.* at col. 6:60-67].[6]

[6] *See also* Ex. O at p. 5 [*Live Traffic Analysis* paper] ("The distribution of recently observed values is evaluated against the long-term profile, and a distance between the two is obtained. The difference is compared to a historically adaptive, subject-specific deviation. The empirical distribution of this deviation is transformed to obtain a score for the event. Anomalous events are those whose scores exceed a historically adaptive, subject specific threshold score based on the empirical score distribution.").

The specification makes clear that the threshold for identifying suspicious network activity must be a historically adaptive threshold that is empirically determined by the network monitor, not a fixed threshold set by a network administrator. According to the specification, "By comparing the long-term and short-term statistical profiles, a monitor can distinguish between normal error levels indicative of intrusion ***without*** burdening a network administrator with the task of arbitrarily ***setting an unvarying threshold***." (Ex. C at col. 13:22-27 ['338 patent] (emphasis added).) Moreover, the specification distinguishes threshold analysis that detects when the number of occurrences of an event (e.g., failed login requests) exceeds a fixed threshold number as a signature detection method, not a statistical detection method. (Ex. C at col. 7:46-50 ['338 patent]; [redacted].) The determination of whether the difference between the long-term and short-term statistical profiles constitutes suspicious network activity "require[s] no a priori knowledge of intrusive or exceptional activity" (Ex. C at col. 6:57-58 ['338 patent]; [redacted].)

Based upon the description in the specification, Defendants therefore propose that the term "determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity" be construed to mean "determining whether the difference between the short-term statistical profile and the long-term statistical profile exceeds a threshold that is empirically determined to indicate suspicious activity based on the historically adaptive deviation between the two profiles, requiring no prior knowledge of suspicious network activity."

SRI's Proposed Construction

SRI contends that these terms do not require construction, and argues in the alternative for a construction that lacks any requirement that the difference between the short-term and long-term profiles exceed a difference which is historically adaptive for the monitored network. SRI's construction would appear to encompass determinations of suspicious network activity based on fixed thresholds reflecting prior knowledge of differences that indicated suspicious network activity. For example, under SRI's construction, the user, not the system, could set a threshold value for identifying suspicious activity (e.g., suspicious activity if short-term statistical profile exceeds long-term statistical profile by fixed value X). But as shown above, the specification instructed one of ordinary skill in the art that the claimed statistical detection step was different than signature detection because it ***did not use*** fixed threshold values reflecting prior knowledge of suspicious activity on the monitored network. Because SRI's proposed construction fails to make this important distinction, it should be rejected.

F. "Statistical detection method"

Claim Term	Defendants' Proposed Construction
"statistical detection method"	a method of detecting suspicious network activity which comprises building a *long-term statistical profile* and a *short-term statistical profile*. This method requires no prior knowledge of suspicious network activity. This method is not a signature matching detection method or threshold analysis.

The claims distinguish between statistical detection methods and signature detection methods. (*Compare* '212 claim 1 *with* '212 claims 2 and 3.) The specification also describes statistical analysis as being distinct from signature analysis. (Ex. C at col. 4:50-53 ['338 patent].) Therefore, at a minimum, a statistical detection method is not a signature matching detection method that uses a fixed threshold because a statistical detection method requires no prior knowledge of suspicious network activity. (*See* Ex. C at col. 6:54-58 ['338 patent]; Ex. I at pp. 481:19-482:4 [Kesidis Dep.]; [redacted].)

However, beyond distinguishing between statistical detection methods and signature detection methods, the specification provides little additional guidance beyond the single example of building and comparing long-term and short-term statistical profiles. There is no evidence that the term "statistical detection method" had a common or ordinary meaning to persons of ordinary skill in the art as of November 1998. [redacted] Similarly, SRI's expert testified that there was "a gray area, I think, between the two definitions." (Ex. I at pp. 477:2-478:11 [Kesidis Dep.].) [redacted]

Given that the specification only discloses a single example of a statistical detection method, the absence of any well-understood ordinary meaning for the term, and the inability of the inventors to identify other known statistical detection methods as of the filing date of the patents, the ***only*** statistical detection method described in the specification is the use of long-term and short-term statistical profiles to detect suspicious network activity. *See Digital Biometrics, Inc. v. Identix, Inc.* 149 F.3d 1335, 1344 (Fed. Cir. 1998) ("[I]f the claim is susceptible to a broader and a narrower meaning, and the narrower one is clearly supported by the intrinsic evidence while the broader one raises questions of enablement under § 112, ¶ 1, we will adopt the narrower of the two."); *Lizardtech, Inc. v. Earth Resource Mapping, Inc.*, 433 F.3d 1373, 1375 (Fed. Cir. 2006) (denial of petition for rehearing en banc) (Lourie, J. concurring) ("Claims are not necessarily limited to preferred embodiments, but, if there are no other embodiments, and no other disclosure, then they may be so limited.")

Accordingly, Defendants propose that the term "statistical detection method" should be construed to be limited to (a) building and using a long-term and short-term statistical profile to detect suspicious network activity, (b) requiring no prior knowledge of suspicious network activity, and (c) not encompassing signature detection methods or threshold analysis.

SRI's Proposed Construction

SRI argues that that there is no need to construe the "statistical detection method" limitation, and argues in the alternative for a construction that would not require the use of a difference that is historically adaptive for the monitored network. This proposal, however, would again fail to inform the jury of a critical distinction drawn by the specification between the "statistical detection method" and the "rudimentary, inexpensive signature analysis technique" of using unvarying thresholds that reflect prior knowledge of suspicious network activity. Defendants' construction of "statistical detection method" should therefore be adopted.

VI. CONCLUSION

For the foregoing reasons, Defendants respectfully request that the Court adopt Defendants' claim constructions.

POTTER ANDERSON & CORROON LLP

By: */s/ David E. Moore*
Richard L. Horwitz (#2246)
David E. Moore (#3983)
Hercules Plaza 6th Floor
1313 N. Market Street
Wilmington, DE 19801
Tel: (302) 984-6000
rhorwitz@potteranderson.com
dmoore@potteranderson.com

OF COUNSEL:

Holmes J. Hawkins III
Natasha H. Moffitt
KING & SPALDING LLP
191 Peachtree Street
Atlanta, GA 30303
Tel: (404) 572-4600

Theresa A. Moehlman
KING & SPALDING LLP
1185 Avenue of the Americas
New York, New York 10036
Tel.: (212) 556-2100

Attorneys for Defendants
Internet Security Systems, Inc., a Delaware Corporation; and Internet Security Systems, Inc., a Georgia corporation

MORRIS JAMES HITCHENS & WILLIAMS LLP

By: */s/ Mary B. Matterer*
Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
Tel.: (302) 888-6800
rherrmann@morrisjames.com
mmatterer@morrisjames.com

OF COUNSEL:

Lloyd R. Day, Jr.
Robert M. Galvin
Paul S. Grewal
DAY, CASEBEER MADRID & BATCHELDER LLP
20300 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: (408) 873-0110

Michael J. Schallop
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: (408) 517-8000

Attorneys for Defendant
Symantec Corporation

Dated: June 9, 2006
Public Version Dated: June 20, 2006

735928

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

CERTIFICATE OF SERVICE

I, David E. Moore, hereby certify that on June 20, 2006, the foregoing document was hand delivered to the following persons and was electronically filed with the Clerk of the Court using CM/ECF which will send notification of such filing(s) to the following and the document is available for viewing and downloading from CM/ECF:

John Horvath
Fish & Richardson P.C.
919 N. Market Street, Suite 1100
P. O. Box 1114
Wilmington, DE 19899

Richard K. Herrmann
Morris James Hitchens & Williams LLP
222 Delaware Avenue, 10th Floor
P.O. Box 2306
Wilmington, DE 19899-2306

I hereby certify that on June 20, 2006, I have Federal Expressed the attached document to the following non-registered participants:

Howard G. Pollack
Michael J. Curley
Fish & Richardson P.C.
500 Arguello Street, Suite 500
Redwood City, CA 94063
pollack@fr.com
curley@fr.com

Paul S. Grewal
Day Casebeer Madrid & Batchelder LLP
20300 Stevens Creek Boulevard
Suite 400
Cupertino, CA 95014
pgrewal@daycasebeer.com

/s/ David E. Moore
Richard L. Horwitz
David E. Moore
POTTER ANDERSON & CORROON LLP
Hercules Plaza, 6th Floor
1313 North Market Street
Wilmington, DE 19899-0951
(302) 984-6000
rhorwitz@potteranderson.com
dmoore@potteranderson.com